Charles H. Thronson, USB 3260
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, UT 84111
Telephone: (801) 532-1234
Facsmile: (801) 536-6111
cthronson@parsonsbehle.com

William B. Federman*
Oklahoma Bar No. 2853
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

A. Brooke Murphy*
Oklahoma Bar No. 30187
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73120
Telephone: (405) 389-4989
abm@murphylegalfirm.com

**Pro Hac Vice* application to be submitted

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

VICTOR SANCHEZ, individually and on behalf of all others similarly situated, Plaintiff, v. SNAP FINANCE LLC and SNAP RTO LLC, Defendants.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Victor Sanchez ("Plaintiff") individually and on behalf of all others similarly situated, and by and through his undersigned counsel files this Class Action Complaint against Defendants Snap Finance LLC and Snap RTO LLC (collectively, "Defendants" or Snap) and allege the following based upon personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Defendants provide financing services, including "lease to own" contracts. To provide these services and in the ordinary course of Snap's business, Defendants acquires, processes, analyzes, and otherwise utilizes the personally identifiable information ("PII") of their customers and applicants, including, but not limited to, their names and Social Security numbers.

2. By taking possession and control of Plaintiff's and Class members' PII, Defendants assumed a duty to securely store and protect that sensitive information.

3. Defendants breached this duty and betrayed the trust of their clients, Plaintiff and Class members by failing to properly safeguard and protect their PII, thus enabling cybercriminals to steal and misuse it.

4. With this action, Plaintiff and the Class seek to hold Defendants responsible for the harms they caused them resulting from the massive and preventable disclosure of such sensitive and personal information.

5. On or about June 23, 2022, cybercriminals foreseeably accessed files on Defendants' network containing the PII of Plaintiff and thousands of other Class Members (the "Data Breach"). This unauthorized and relatively unfettered access by cybercriminals lasted for more than two months, ending only on September 8, 2022. Defendants' monitoring practices

were so poor that they did not identify this intrusion until months after they began. On October 28, 2022, Snap determined through their investigation into the Data Breach that the PII of 61,302 customers was affected.[1] Snap then inexplicably waited until December 1, 2022, to begin notifying victims of the Data Breach.

6. As a result of Defendants' negligent and wrongful conduct, Plaintiff's and Class members' valuable PII was left in the hands of cybercriminals.

7. Defendants' misconduct—failing to implement adequate and reasonable data security measures to protect Plaintiff's and Class members' PII, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that they did not have adequate security practices and employee training in place to safeguard the PII, failing to honor their promises and representations to protect Plaintiff's and Class members' PII, and failing to provide timely and adequate notice of the Data Breach—caused substantial harm and injuries to Plaintiff and Class members across the United States.

8. Due to Defendants' negligence and data security failures, cybercriminals had access to, and now potentially possess, everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

9. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that Plaintiff's PII has been released to cybercriminals, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/d193f4eb-a877-4395-9a3c-8b94833c907c.shtml.

identity thieves possessing and fraudulently using their PII. Plaintiff and Class members have lost time and money responding to and attempting to mitigate the impact of the Data Breach.

10. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages, statutory damages, treble damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security protocols and employee training practices), reasonable attorney's fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

THE PARTIES

11. Plaintiff is a citizen and resident of the state of Nevada. Plaintiff received a letter from Snap, notifying him that his PII, including his Social Security number and driver's license number, had been compromised in the Data Breach.

12. Defendant Snap Finance LLC is a Utah limited liability company with its principal place of business in South West Valley, Utah.

13. Defendant Snap RTO LLC is a Utah limited liability company with its principal place of business in South Salt Lake City, Utah.

JURISDICTION AND VENUE

14. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendants.

15. This Court has personal jurisdiction over Defendants because Defendants is headquartered in this District and Defendants conducts substantial business in Utah and this District through their headquarters and offices.

16. Venue is likewise proper as to Defendants in this District under 28 U.S.C. § 1391 because Defendants is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

17. For Snap to perform their financing services, from which they generate their profits, Defendants collects and stores the PII of individuals, including Plaintiff and the Class.

18. Due to the highly sensitive and personal nature of the information Defendants acquires and stores with respect to loan applicants and customers, Defendants recognizes the privacy rights of the individuals whose PII Defendants obtains, as evidenced by Snap's publicly available privacy policy ("Privacy Notice").[2] Defendants' Privacy Notice promises to, among other things, that:

> Snap stores and processes your information maintaining physical, electronic and procedural safeguards. We maintain physical security measures to guard against unauthorized access to systems and use safeguards such as firewalls and data encryption. We enforce physical access controls to our buildings, and we authorize access to personal information only for those employees or contractors who require it to fulfill the responsibilities of their jobs.

[2] https://snapfinance.com/legal/privacy.

19. Plaintiff and the Class Members reasonably expected that Defendants would implement and maintain reasonable data security measures to protect their PII from foreseeable threats.

20. Earlier this year, Snap became aware of a data security incident that impacted its network, indicating a likely data breach. Based on a forensic investigation, Snap confirmed that cybercriminals had infiltrated its systems and were active on its network between June 23, 2022 and September 8, 2022. During this time, cybercriminals had unauthorized and undetected access to certain sensitive information, including the PII of 61,302 individuals, including names, Social Security numbers, driver's license numbers, and financial account numbers.

21. On information and belief, the PII accessible to cybercriminals was not encrypted.

22. On information and belief, the cyberattack was targeted at Defendants due to their status as a major loan provider that obtains and stores large amounts of PII.

23. On information and belief, the targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including the PII of Plaintiff and the Class members.

24. Moreover, while Defendants admits that they learned of the Data Breach in October 2022, Defendants inexplicably waited until December 2022 before they began the process of notifying impacted individuals, such as Plaintiff and Class members.

25. Due to Defendants' inadequate security measures and their delayed notice to victims, Plaintiff and the Class members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

26. Defendants had obligations created by industry standards, common law, and their own promises and representations made to Plaintiff and Class members to keep their PII confidential and to protect it from unauthorized access and disclosure.

27. Plaintiff and Class Members had the reasonable expectation that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

29. As a result of Defendants' negligent and wrongful conduct, Plaintiff's and Class members' sensitive PII was left exposed to cybercriminals.

B. Plaintiff's Experience

30. Plaintiff received a letter from Snap in December 2022, advising him that his PII, including his name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

31. Because of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff's PII has been obtained by cybercriminals.

32. Plaintiff is now under an imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff's life. The imminent risk of identity theft and fraud Plaintiff now faces is substantial, certainly impending, continuous, and ongoing because of

the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

33. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff, including (but not limited to) investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, reviewing accounts statements, and monitoring other personal information.

34. As a direct and proximate result of the Data Breach, Plaintiff will need to have identity theft protection for the foreseeable future.

35. Plaintiff has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff's PII. Additionally, Plaintiff's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

C. Defendants was on Notice of Data Threats in the Industry and of the Inadequacy of their Data Security

36. Defendants was on notice that companies maintaining large amounts of PII are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information.

37. At all relevant times, Snap knew, or should have known, that the PII that they collected was a target for malicious actors. Despite such knowledge, Snap failed to implement and

maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Snap should have anticipated and guarded against.

38. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . Many of them were caused by flaws in . . . systems either online or in stores."[3]

39. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Snap knew or should have known that their electronic records would be targeted by cybercriminals.

40. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

41. Moreover, PII is a valuable property right.[4] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data

[3] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[4] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

within the existing legal and regulatory frameworks."[5] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[6] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

42. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

43. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[7]

---

[5] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[6] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[7] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

44. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Cyber Criminals Will Use Plaintiff's and Class Members' PII to Defraud Them

45. Plaintiff's and Class members' PII is of great value to cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

46. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[8] For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[9] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

[8] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").
[9] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

47. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[10]

48. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[11]

49. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[12]

50. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

[10] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.
[11] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.
[12] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.
[13] *Data Breaches Are Frequent*, *supra* note 11.

51. For instance, with a stolen Social Security number, which is only one category of the PII compromised in the Data Breach, someone can open financial accounts, file fraudulent tax returns, commit crimes, and steal benefits.[14]

52. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[15]

53. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other information for unauthorized activity for years to come.

54. Plaintiff and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

[14] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[15] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential information used against them by spam callers to defraud them;

e. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

55. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Defendants, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant

security measures and safeguards. Defendants has shown themselves to be wholly incapable of protecting Plaintiff's and Class members' PII.

56. Plaintiff and Class members are desperately trying to mitigate the damage that Defendants has caused them but, given the kind of PII Defendants made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PII, Plaintiff and Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[16]

57. None of this should have happened. The Data Breach was entirely preventable.

E. Defendants Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' PII

58. Data disclosures and data breaches are preventable.[17] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[18] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[19]

---

[16] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.
[17] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[18] *Id.* at 17.
[19] *Id.* at 28.

59. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[20]

60. Defendants obtained and stored Plaintiff's and Class members' PII—including but not limited to, their names Social Security numbers—and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII.

61. Defendants breached fiduciary duties owed to Plaintiff and the Class as guardian of their PII.

62. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendants' failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiff's and Class members' PII.

63. Defendants maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

64. Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class members' PII was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

[20] *Id.*

65. The risk of improper disclosure of Plaintiff's and Class members' PII was a known risk to Defendants, and thus Defendants was on notice that failing to take necessary steps to secure Plaintiff's and Class members' PII from that risk left the PII in a dangerous condition.

66. Defendants disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

67. Plaintiff brings this action under Federal Rule of Civil Procedure 23 against Defendants individually and on behalf of all others similarly situated. Plaintiff asserts all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose personally identifiable information was accessed or acquired as a result of the Snap data breach that is the subject of the notice of Data Breach that Defendants sent to Plaintiff and other Class Members (the "Nationwide Class" or "Class").

68. Excluded from the Nationwide Class are Defendants, any entity in which Defendants has a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or

judicial officer presiding over this matter and members of their immediate families and judicial staff.

69. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

70. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

71. Numerosity: The proposed Class is believed to be so numerous that joinder of all members is impracticable.

72. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendants.

73. Adequacy: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class he seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

74. Superiority: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not

impossible, for members of the Class individually to effectively redress Defendants' wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

75. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;
b. Whether Defendants failed to adequately safeguard Plaintiff's and the Class's PII;
c. Whether Defendants' computer systems and data security practices used to protect Plaintiff's and Class members' PII violated the FTC Act, and/or state laws and/or Defendants' other duties discussed herein;
d. Whether Defendants owed a duty to Plaintiff and the Class to adequately protect their PII, and whether they breached this duty;
e. Whether Defendants knew or should have known that their computer and network security systems and business email accounts were vulnerable to a data breach or disclosure;
f. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendants breached contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

h. Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate they diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Plaintiff and the Class suffered injury as a proximate result of Defendants' negligent actions or failures to act;

j. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class;

and

l. Whether Plaintiff and Class members are entitled to treble damages.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

76. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

77. Defendants gathered and stored the PII of Plaintiff and the Class as part of the operation of their business.

78. Upon accepting and storing the PII of Plaintiff and Class members, Defendants undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure

and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

79. Defendants had full knowledge of the sensitivity of the PII, the types of harm that Plaintiff and Class members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

80. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their PII that was in Defendants' possession. As such, a special relationship existed between Defendants and Plaintiff and the Class.

81. Defendants owed Plaintiff and Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their PII, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

82. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

83. Defendants had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendants owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' PII in their possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and Class members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

84. Only Defendants was in a position to ensure that their systems and protocols were sufficient to protect the PII that had been entrusted to it.

85. Defendants breached their duties of care by failing to adequately protect Plaintiff's and Class members' PII. Defendants breached their duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in their possession;

b. Failing to protect the PII in their possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train their employees regarding how to properly and securely transmit and store PII;

d. Failing to adequately train their employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PII;

f. Failing to mitigate the harm caused to Plaintiff and the Class members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their PII.

86. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

87. As a proximate and foreseeable result of Defendants' negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

88. Through Defendants' acts and omissions described herein, including but not limited to Defendants' failure to protect the PII of Plaintiff and Class members from being stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members while it was within Defendants' possession and control.

89. Further, through their failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendants prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their PII and mitigate damages.

90. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the PII, and closely reviewing and monitoring bank accounts, credit reports, and financial statements.

91. Defendants' wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

92. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' negligent conduct.

93. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

94. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

95. In connection with the dealings Plaintiff and Class Members had with Snap, Plaintiff and Class members entered into implied contracts with Snap.

96. Pursuant to these implied contracts, Plaintiff and Class members provided Snap with their PII in order for Snap to provide financing services. In exchange, Snap agreed to, among other things, and Plaintiff and Class members understood that Snap would: (1) provide services to

Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members PII in compliance with federal and state laws and regulations and industry standards.

97. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Snap, on the other hand. Indeed, Snap was clear in its Privacy Policy, and Plaintiff understood, that Snap supposedly respects and is committed to protecting customer privacy.

98. Had Plaintiff and Class members known that Snap would not adequately protect its clients' customers' and former customers' PII, they would not have provided Snap or Snap's clients with their PII.

99. Plaintiff and Class members performed their obligations under the implied contracts when they provided Snap with their PII, either directly or indirectly.

100. Snap breached its obligations under their implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

101. Snap's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

102. Plaintiff and all other Class members were damaged by Snap's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not

receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

Third Cause of Action
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

103. Plaintiff reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

104. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

105. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

106. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

107. Moreover, Defendant retained the PII with no legitimate employment or business purpose.

108. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures.

Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

109. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

110. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

111. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant or would have requested that the PII be deleted upon termination of the employment or business relationship.

112. Plaintiff and Class Members have no adequate remedy at law.

113. As a direct result of the Data Breach, Plaintiff and Class Members have suffered the following actual and imminent injuries: (a) monetary harms, including out-of-pocket expenses, loss-of time, and loss of productivity incurred mitigating the present risk and imminent threat of identity theft; (b) actual identity theft and fraud resulting in additional monetary damages; (c) diminution of value of their PII; (d) anxiety, stress, nuisance, and annoyance; (e) increased targeted and fraudulent robocalls and phishing email attempts; (f) the present and continuing risk of identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) the retention of the reasonable value of the PII entrusted to Defendant; and (h) the present and continued risk to PII, which remains on Defendant's vulnerable networks, placing Plaintiff and Class Members at an ongoing risk of harm.

114. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

115. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FOURTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

117. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

118. Defendants owed and owes a duty of care to Plaintiff and Class members that require they to adequately secure Plaintiff's and Class members' PII.

119. Defendants still possesses the PII of Plaintiff and the Class members.

120. Defendants has not satisfied their contractual obligations and legal duties to Plaintiff and the Class members.

121. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

122. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

123. Plaintiff and the Class, therefore, seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants provide employee training regarding the dangers and risks inherent in using file-sharing websites;

e. Ordering that Defendants cease transmitting PII via file-sharing websites;

f. Ordering that Defendants cease storing PII on file-sharing websites;

g. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for their provision of services;

h. Ordering that Defendants conduct regular database scanning and security checks; and

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendants as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, treble damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: December 21, 2022

/s/ Charles H. Thronson

Charles H. Thronson, USB 3260
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, UT 84111
Telephone: (801) 532-1234
Facsimile: (801) 536-6111
CThronson@parsonsbehle.com

William B. Federman, OSB 2853 *
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

A. Brooke Murphy, OSB 30187 *
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

**pro hac vice request* forthcoming

Counsel for Plaintiff and the Putative Class